IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Antonio Lain and Viacheslav Borisov		
Assignee:	Hewlett-Packard Development Company, L.P.		
Title:	Cryptographic Key Update Management Method and Apparatus		
Serial No.:	10/814,608	Confirmation No.	5425
Docket No.:	200310005-2	Filing Date:	March 30, 2004
Examiner:	Bryan F. Wright	Group Art Unit:	2431

February 16, 2011

Mail Stop APPEAL BRIEF
COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. §§ 1.191 AND 41.67

Dear Sir:

Appellants submit this Appeal Brief pursuant to the Notice of Appeal filed in the above-identified patent application on December 16, 2010.

I. REAL PARTY IN INTEREST

The real party in interest is the assignee, Hewlett-Packard Development Company, L.P., as named in the caption above.

II. RELATED APPEALS AND INTERFERENCES

Based on information and belief, there are no prior or pending appeals, interferences or judicial proceedings known to Appellants, the Appellants' legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

III. STATUS OF CLAIMS

Claims 1-21, which are reproduced in an Appendix below, are pending in this case, stand rejected, and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

There are no unentered amendments in this case. No amendments were filed subsequent to the Final Rejection dated September 16, 2010.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Appellants' application discloses techniques for enabling secure communications among members of a group using a logical key hierarchy ("LKH") such as LKH 120 in Fig. 2 of the application. Such a hierarchy may be established for clients that are associated with respective leaf keys of the hierarchy, and each client may know its leaf key and all the other keys in the path from that leaf key to the root key of the LKH. The root key of the LKH may be a group key and may be used to encrypt and send a secure message to all the clients in the group. As described on page 1 of Appellants' specification, the keys may be updated to maintain security when a client joins or leaves the group. Updating may involve sending update records to the current clients. The subject matter on appeal addresses the problem of how to update a client that has missed one or more updates. For instance, an entity (e.g., KHT cache 20 in Fig. 1 of Appellants' specification) may receive all update records and consolidate the update records into a "key history tree" (KHT) that a re-connecting client can use to update the set of keys that the client is authorized to have.

Independent claim 1 specifically recites "Apparatus for consolidating key updates generated for members of a group." An example of such apparatus is KHT cache 20 of Fig. 1, which is introduced in the paragraph beginning at page 5, line 4. As recited in claim 1, "the key updates are provided in records that each comprise an encrypted key corresponding to a node of a key hierarchy and encrypted using a key that corresponds to a descendant of that node, hierarchy-node information for both the encrypted and encrypting keys, and key-version information for at least the encrypted key." Such records are illustrated by update records 18 in Fig. 1. (See also page 7, lines 20-26 and page 8, lines 7-16 for a description of record content.) Claim 1 further recites that the apparatus includes "a communications interface for receiving said records and a manager," e.g., communication interface 21 and manager 22 of Fig. 1. For the manager, claim 1 recites, "maintaining, on the basis of the received records, a key history tree," which corresponds in an illustrated embodiment to key history tree 24 of Fig. 1. "A key tree with nodes corresponding to nodes in said hierarchy" is described beginning at page 9, line 19. Claim 1 finally recites "the manager being arranged to store in association with each tree node, for each encrypting key used in respect of the encrypted key

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded." An example of the maintenance of a key history tree containing encrypted keys is illustrated in Fig. 3, and description of operation of a manager to store and overwrite nodes of a key history tree begins at page 9, line 31. More particularly, storing up-to-date encrypted keys at nodes is described, for example, in the paragraph beginning at page 10, line 1. Discarding earlier versions is described, for example, at page 10, lines 31 to page 11, line 2.

Independent claim 13 recites, "A method of consolidating key updates provided in records each comprising an encrypted key corresponding to a node of a key hierarchy and encrypted using a key that corresponds to a descendant of that node, hierarchy-node information for both the encrypted and encrypting keys, and key-version information for at least the encrypted key." Key updates and their contents are described in page 7, lines 20-26 and page 8, lines 7-16. Claim 13 further recites, "the method comprising ... maintaining in a computer system, on the basis of said records, a key history tree with tree nodes corresponding to nodes in said hierarchy." An example of the maintenance of a key history tree is illustrated in Fig. 3, and description of operation of a manager for a key history tree can be found beginning at page 10, line 1. Claim 13 finally recites, "this tree-maintenance step comprising ... storing in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded." Storing up-to-date encrypted keys at nodes is described, for example, in the paragraph beginning at page 10, line 11. Discarding earlier versions is described, for example, at page 10, line 31 to page 11, line 2.

Claim 21 recites, "A method of providing key updates to members of a group, comprising the steps of: managing a key hierarchy in dependence on the addition and/or removal of members to said group." Managing a key hierarchy, e.g., LKH, is illustrated in Fig. 2 and described beginning at page 5, line 24. The step of "outputting, as notification of the changes made to the key hierarchy, records that each comprise an encrypted key corresponding to a node of the key hierarchy and encrypted using a key which is a descendant of that node, and hierarchy-node and key-version information for both the encrypted and encrypting keys" is described, for example, at page 8, lines 7-17. Claim 21 further recites, "consolidating said records according to the method of claim 13." The method of claim 13 is summarized above with references to page and line numbers in the specification. Claim 21

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

finally recites, "providing said key tree, or a subset of it, to members of said group whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin." See the paragraph beginning at page 9, line 10 of Appellants' specification.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following rejections are presented to the Board of Patent Appeals and Interferences for decision:

A. Claims 1-4, 8, 12-16, and 20 stand rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Pat. App. Pub. No. 2002/0059286 (hereinafter Challener) in view of U.S. Pat. No. 6,049,878 (hereinafter Caronni) and further in view of U.S. Pat. No. 6,363,149 (hereinafter Candelore).

B. Claims 5-7, 9-11, 17-19, and 21 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Challener in view of Caronni and Candelore and further in view of U.S. Pat. App. Pub. No. 2003/0126464 (hereinafter McDaniel).

VII. ARGUMENT

A. Claims 1-4, 8, 12-16, and 20 are patentable under 35 U.S.C. § 103(a) over Challener in view of Caronni and Candelore.

Appellants note section 2, on page 2 of the Final Office Action sets forth a rejection under 35 U.S.C. § 103(a) but does not mention claims 8 and 20. However, section 7, beginning on page 7 of the Final Office Action, identifies claims 8 and 20 and relates the limitations of claims 8 and 20 to the combined teachings of Challener, Caronni, and Candelore. Appellants, therefore are interpreting the Final Office Action as rejecting claims 8 and 20 under 35 U.S.C. 103(a), and the following remarks are based on that interpretation.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

Independent claim 1 distinguishes over the combination of Challener, Caronni, and Candelore at least by reciting, "a manager for maintaining, on the basis of the received

records, a key history tree with tree nodes corresponding to nodes in said hierarchy, the manager being arranged to store in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded." The combination of Challener, Caronni, and Candelore fails to suggest such a manager as recited in claim 1.

Challener is directed to trusted computing platforms, which in order to comply with Trusted Computing Platform Alliance (TCPA) standard must use 2048-bit RSA strings in a tree structure. Challener is particularly concerned with the 2048 bit lengths of the strings required by the TCPA standard because the long keys make some manipulations slow. See paragraphs [0003] and [0004] of Challener. Challener teaches that use of a second tree structure that matches TCPA tree but contains keys of other types that require less time to manipulate, can improve performance of a trusted computing platform. Neither of the tree structures disclosed by Challener are related to key updates or consolidation of key updates used for secure group communications. Challener does not teach or suggest key updates or a key history tree.

Caronni is directed to multicasting of data to group members or participants and discloses use of a hierarchy of encryption keys, where each key has version information, i.e., a version number and a revision number. The version number and revision number that Caronni discloses can be used when sending key updates or heartbeat messages to participants. See, for example, Caronni, column 6, lines 37-39. As described by Caronni, participants can update their keys using the revision number and a one-way hash function when a participant is added to the group, but when a participant is deleted from the group, the version number changes, and a participant remaining in the group requires new keys. A remaining participant may receive version updates directly from the group manager or from a log of version updates if the member missed one or more update messages. Caronni does not suggest a manager that maintains a key history tree where earlier versions of a key may be discarded.

Candelore is directed to a system for accessing encrypted data such as encrypted digital video. In accordance with the teaching of Candelore, a system for decoding video or other data may use a sequence of keys during respective time periods during which the system is entitled to decrypt data, and a system may not receive a key for particular time periods if the system is not entitled to decrypt data, e.g., if a fee has not been paid. Candelore further

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

describes techniques for which a system can recover a key or keys using a one-way function and one or more entitlement messages. Candelore is not directed to a system having keys with a tree hierarchy and does not suggest a manager that maintains a key history tree based on records where earlier versions of a key may be discarded.

The rejection of claim 1 in the Final Office Action is in error at least because Challener, Caronni, and Candelore, whether considered separately or in combination provide no suggestion of a manager that maintains a key history tree based on records where an up-to-date version of a key is stored and where any earlier versions are discarded. As disclosed in Appellants' specification use of a key history tree of the recited type may permit recovery from missed updates without requiring maintenance of a log of all update messages. In particular, discarding earlier versions may allow the tree history to be smaller and less complex than a log of all update messages would be after several members leave a group.

In regard to a manager as recited in claim 1, the Final Office Action beginning in the last paragraph of page 3 cites Caronni (and particularly Caronni, col. 10, lines 1-12) as teaching or suggesting a manager for maintaining, on the basis of received records means for updating key data. Caronni, col. 9, line 66 to col. 10, line 2 describes that multiple "joins" and/or "leaves" (i.e., events when multiple members join or leave the group) may be simultaneously processed into a single update message. This portion of Caronni thus teaches a method for generating an update message based on multiple changes in the content of the group. This is quite different from a manager consolidating or maintaining a history based on records in which the update messages are provided. Caronni, col. 10, lines 2-12 further summarizes how revision numbers are used when members join the group and version numbers are used when members leave the group. Caronni does describe that "If a participant missed some version changes, he must ask any member of the group or the group manager to provide him with a log of key version change messages." Thus, to avoid a member needing to rejoin the group, Caronni describes that a log or list of all of the version update messages can be provided to an out-of-date group member. Caronni does not describe or suggest maintaining a "key history tree" as recited in claim 1 or a "manager being arranged to store in association with each tree node … the most up-to-date version of the encrypted key … with any earlier versions being discarded."

Caronni (unlike Challener) does describe a system using key updates, but Caronni still fails to suggest consolidation of such updates to maintain a key history (and more particularly key history tree) based on key updates. The Final Office Action at page 4, lines 15-16 states

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

that "a key history tree is simply a cache (e.g., storage) that enables a previous key to be derived." However, claim 1 recites "a key history tree with tree nodes corresponding to nodes in said hierarchy, … arranged to store in association with each tree node … the most up-to-date version of the encrypted key and its version information." Thus, claim 1 does not call simply for a general cache, log, or storage but instead requires a "key history tree" with nodes according to the key hierarchy. Caronni describes only a log of key updates. Candelore is cited for teaching a method for obtaining previous key data from storage, but Candelore is directed to an ordered sequence of key, not a tree hierarchy. Combining Candelore with Caronni and Challener fails to suggest maintaining a key history tree.

In Graham v. John Deere Co. of Kansas City, 383 U. S. 1, 17-18 (and more recently in KSR International Co. v. Teleflex Inc., 550 USPQ2d 1385 (2007), the U.S. Supreme Court set forth analysis used in applying 35 U.S.C. §103. In accordance with Graham, "the scope and content of the prior art are ... determined; differences between the prior art and the claims at issue are ... ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined." In the present case, the combination of Challener, Caronni, and Candelore at best discloses maintaining a log or ordered sequence of updates. In contrast, claim 1 recites, "a key history tree with tree nodes corresponding to nodes in said hierarchy, the manager being arranged to store in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded." The use of a tree structure for a key history and discarding of earlier versions of keys would not have been obvious to one of ordinary skill in the art in view of Challener, Caronni, and Candelore. Accordingly, claim 1 is patentable over under 35 U.S.C. § 103(a) over Challener in view of Caronni and Candelore.

Claims 2-4, 8, and 12 depend from claim 1 and are patentable over Challener, Caronni, and Candelore for at least the same reasons that claim 1 is patentable over Challener, Caronni, and Candelore.

Independent claim 13 distinguishes over the combination of Challener and Caronni at least by reciting, "maintaining … on the basis of said records, a key history tree … this tree-maintenance step comprising … storing in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

discarded.." As noted above, the combination of Challener, Caronni, and Candelore fails to disclose or suggest these features of independent claim 13. Accordingly, claim 13 is patentable over Challener in view of Caronni and Candelore.

Claims 14-16 and 20 depend from claim 13 and are patentable over Challener, Caronni, and Candelore for at least the same reasons that claim 13 is patentable over Challener, Caronni, and Candelore.

B. Claims 5-7, 9-11, 17-19, and 21 are patentable under 35 U.S.C. 103(a) over Challener in view of Caronni, Candelore, and McDaniel.

Claims 5-7 and 9-11 depend from claim 1 and are patentable over the combination of Challener, Caronni, and Candelore for the reasons given above to show claim 1 is patentable. McDaniel is directed to enforcing security policies and describes re-keying as one process that a security policy may require. However, McDaniel does not cure the deficiencies of Challener, Caronni, and Candelore noted above. Accordingly, the above reasoning showing claim 1 is patentable over Challener, Caronni, and Candelore also applies to the combination of Challener, Caronni, Candelore, and McDaniel, and claim 1 and claims 5-7 and 9-11, which depend from claim 1, are patentable over the combination of Challener, Caronni, Candelore, and McDaniel.

Claims 17-19 and 21 depend from claim 13 and are similarly patentable over the combination of Challener, Caronni, Candelore, and McDaniel at least because claim 13 recites, "maintaining ... on the basis of said records, a key history tree" and "storing in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded.." Accordingly, claim 13 and claims 17-19 and 21, which depend from claim 13, are patentable over Challener, Caronni, Candelore, and McDaniel.

For the above reasons, Appellants respectfully submit that pending Claims 1-21 are allowable. Accordingly, Appellants submit the present rejections are unfounded and request that the rejections of claims 1-21 be reversed.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

Please contact the undersigned attorney at (530) 621-4545 if there are any questions concerning this Appeal Brief or the application generally.

Respectfully submitted,

/David Millers 37396/

David Millers
Reg. No. 37,396

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

VIII. CLAIMS APPENDIX

Claims 1-21, which are the claims involved in this appeal, are copied below.

1. (Previously Presented) Apparatus for consolidating key updates generated for members of a group, wherein the key updates are provided in records that each comprise an encrypted key corresponding to a node of a key hierarchy and encrypted using a key that corresponds to a descendant of that node, hierarchy-node information for both the encrypted and encrypting keys, and key-version information for at least the encrypted key; the apparatus comprising

a communications interface for receiving said records, and

a manager for maintaining, on the basis of the received records, a key history tree with tree nodes corresponding to nodes in said hierarchy, the manager being arranged to store in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded.

2. (Original) Apparatus according to claim 1, wherein the manager is arranged to store each said most up-to-date version of a said encrypted key by storing the record containing the latter with any previously-stored record that is thereby superseded being discarded.

3. (Original) Apparatus according to claim 1, wherein the manager is arranged to store in association with each tree node, along with the most up-to-date version of the corresponding encrypted key stored for each encrypting key used in respect of that encrypted key, version information for the encrypting key used to encrypt said most up-to-date version of the encrypted key, this version information being included in the record providing said most up-to-date version of the encrypted key.

4. (Original) Apparatus according to claim 3, wherein the manager is arranged to replace the version of the encrypted key stored in association with a tree node for a particular encrypting key, with any subsequently received later version of that key provided the latter has been encrypted with a version of the encrypting key that is the same or later than the version used for encrypting the existing stored encrypted key.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

5. (Previously Presented) Apparatus according to claim 1, further comprising a working-set generator for processing the key history tree to generate a subset of the key history tree enabling, at least within a target failure rate, all clients associated with the key hierarchy to recover the current root key of the latter.

6. (Original) Apparatus according to claim 5, wherein the working set generator comprises control means for receiving feedback on the current root-key recovery failure rate and for controlling the size of said subset to approach the actual failure rate to said target failure rate.

7. (Original) Apparatus according to claim 6, wherein the working set generator further comprises means for determining the likelihood of a tree node being required to enable recovery the current root key, these means being based on at least one of the age of the node, or of an encrypted key associated with it, and an estimate of the number of possible clients that will need the node.

8. (Previously Presented) Apparatus according to claim 1, wherein the manager is arranged to maintain said key history tree only in respect of keys corresponding to the nodes of a predetermined sub-hierarchy of said hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the hierarchy.

9. (Previously Presented) A system comprising apparatus according to claim 1, and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to the group, the key-hierarchy manager being arranged to output said records both to currently available members of said group and to said apparatus as notification of the changes made by the key-hierarchy manager to the key hierarchy, said apparatus being arranged to provide said key history tree, or a subset of it, to members of said group who subsequently become available as a consolidated notification of the changes made by the key-hierarchy manager to the key hierarchy whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

10. (Previously Presented) A system comprising apparatus according to claim 1, and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to the group, the key-hierarchy manager being arranged to output said records to said apparatus, said apparatus being arranged to provide said key history tree, or a subset of it, to members of said group as a consolidated notification of the changes made by the key-hierarchy manager to the key hierarchy whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin.

11. (Previously Presented) A system according to claim 10, wherein the key-hierarchy manager and said apparatus form part of an anonymous group content distribution arrangement; the key history tree, or a subset of it, being sent to group members in association with content encrypted with a key that is one of:

- the key-hierarchy root key, and
- a key encrypted using the key-hierarchy root key and provided in encrypted form along with the encrypted content.

12. (Previously Presented) A system comprising multiple apparatuses according to claim 1, and a key-hierarchy manager for managing said key hierarchy in dependence on the addition and/or removal of members to a group and for outputting key update records reflecting changes made to the key hierarchy; the apparatuses being configured in a multiple-level hierarchical arrangement comprising a first-level apparatus arranged to receive the records output by the key-hierarchy manager, and one or more lower levels of apparatuses each arranged to receive the key history tree, or a subset of it, produced by a said apparatus at the next level up, the apparatuses at the lowest level of the hierarchical arrangement each being arranged to provide its key history tree, or a subset of it, to a respective sub-group of members of said group; the apparatuses at each level of said hierarchical arrangement, other than said first level, each being arranged to maintain its said key history tree only in respect of keys corresponding to the nodes of a respective predetermined sub-hierarchy of said key hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the key hierarchy.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

13. (Previously Presented) A method of consolidating key updates provided in records each comprising an encrypted key corresponding to a node of a key hierarchy and

encrypted using a key that corresponds to a descendant of that node, hierarchy-node information for both the encrypted and encrypting keys, and key-version information for at least the encrypted key; the method comprising a step of maintaining in a computing system, on the basis of said records, a key history tree with tree nodes corresponding to nodes in said hierarchy, this tree-maintenance step comprising a sub-step of storing in association with each tree node, for each encrypting key used in respect of the encrypted key associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded.

14. (Original) A method according to claim 13, wherein in said sub-step each said most up-to-date version of a said encrypted key is stored by storing the record containing the latter with any previously-stored record that is thereby superseded being discarded.

15. (Original) A method according to claim 13, wherein in said sub-step the version information of the encrypting key used to encrypt said most up-to-date version of the encrypted key is stored with the latter.

16. (Original) A method according to claim 13, wherein in said sub-step the version of the encrypted key stored in association with a tree node for a particular encrypting key, is replaced with any subsequently received later version of that key provided the latter has been encrypted with a version of the encrypting key that is the same or later than the version used for encrypting the existing stored encrypted key.

17. (Previously Presented) A method according to claim 13, further comprising the further step of processing the key history tree to generate a subset of the key history tree enabling, at least within a target failure rate, all clients associated with the key hierarchy to recover the current root key of the hierarchy.

18. (Original) A method according to claim 17, wherein the further step comprises receiving feedback on the current root-key recovery failure rate and controlling the size of said subset to approach the actual failure rate to said target failure rate.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

19. (Original) A method according to claim 18, wherein said further step further comprises determining the likelihood of a tree node being required to enable recovery the current root key, this determination being based on at least one of the age of the node, or of an encrypted key associated with it, and an estimate of the number of possible clients that will need the node.

20. (Previously Presented) A method according to claim 13, wherein said key history tree is maintained only in respect of keys corresponding to the nodes of a predetermined sub-hierarchy of said key hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the hierarchy.

21. (Previously Presented) A method of providing key updates to members of a group, comprising the steps of:

managing a key hierarchy in dependence on the addition and/or removal of members to said group and outputting, as notification of the changes made to the key hierarchy, records that each comprise an encrypted key corresponding to a node of the key hierarchy and encrypted using a key which is a descendant of that node, and hierarchy-node and key-version information for both the encrypted and encrypting keys; and

consolidating said records according to the method of claim 13 and providing said key history tree, or a subset of it, to members of said group whereby to enable these members to recover the current root key of the key hierarchy at least within a target failure margin.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH (530) 621-4545
FX (530) 621-4543

IX. EVIDENCE APPENDIX

There is no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or any other evidence entered by the Examiner that Appellants are relying upon in this appeal.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543

X. RELATED PROCEEDINGS APPENDIX

No decisions rendered by a court or the Board of Patent Appeals and Interferences are being submitted.

PATENT LAW OFFICE OF
DAVID MILLERS

1221 SUN RIDGE ROAD
PLACERVILLE, CA 95667

PH: (530) 621-4545
FX: (530) 621-4543